

# 12. CVE, CWE and NVD

## CVEs: Common Vulnerabilities and Exposures

### What Are CVEs?

CVEs are **unique identifiers** for publicly known cybersecurity vulnerabilities. They:

- Provide a **standard naming system** for tracking vulnerabilities
- Make it easy for security tools and professionals to reference the same issue
- Are managed by **MITRE Corporation** with sponsorship from the **U.S. DHS CISA**

### Structure of a CVE Identifier

Example: `CVE-2024-1234`

Part	Meaning
<code>CVE</code>	Prefix (Common Vulnerabilities and Exposures)
<code>2024</code>	Year vulnerability was <i>disclosed</i>
<code>1234</code>	Unique number assigned in that year

- CVEs may be reserved ahead of publication (`RESERVED` state)
- Once vetted, full details are disclosed on [CVE.org](https://cve.org)

### Role of CNAs (CVE Numbering Authorities)

**CNAs** are organizations authorized to:

- Assign CVEs to vulnerabilities they find or manage
- Publish basic CVE metadata

### CNA Examples:

- Software Vendors (e.g., Microsoft, Google, Red Hat)
- CERTs/CSIRTs
- Research groups like ZDI (Zero Day Initiative)

### Criteria to Become a CNA:

- Be capable of handling public disclosures

- Commit to CVE assignment and publication standards
- Support coordination with affected parties
- Apply CVE assignment in a consistent and timely way

👉 Full CNA list: <https://cve.org/PartnerInformation/List>

---

## 📄 CVE Entry Process (Simplified Flow)

1. **Vulnerability Found** → Researcher or vendor identifies an issue
2. **CNA or MITRE Contacted** → Request a CVE ID (if not reserved)
3. **Vulnerability Reviewed** → Validate that it's real, unique, and public
4. **CVE Assigned** → Gets an ID like `CVE-2024-xxxx`
5. **Published on CVE.org** with:
  - Description
  - Affected products/versions
  - References (e.g., vendor patches, advisories)

---

## 🔍 Using the CVE Database

Use <https://cve.org> or <https://nvd.nist.gov>

You can search by:

- CVE ID: `CVE-2023-4863`
- Vendor/product: `Apache Log4j`
- Keyword: `RCE` or `SQL injection`
- Date ranges

---

## 🌟 CWEs: Common Weakness Enumeration

### ✅ What Are CWEs?

- **CWEs** describe *types of flaws* in code that can lead to vulnerabilities.
- A **CWE is like a pattern** or blueprint of a vulnerability.
- Managed by **MITRE**, just like CVEs.

💡 **CWE describes the weakness**, while **CVE names a specific instance** of that weakness.

---

## 📁 CWE Categories, Types & Hierarchy

CWEs are structured in a tree-like hierarchy:

Level	Description	Example
Category	Group of related weaknesses	CWE-119: Buffer Errors
Class	Abstract weakness definition	CWE-120: Buffer Overflow
Base	Detailed weakness with technical cause	CWE-78: OS Command Injection
Variant	Specific coding issue	CWE-89: SQL Injection

### Relationship Between CVEs and CWEs

A **CVE entry** typically links to one or more CWEs to describe the **underlying cause**.

**Example:**

```
CVE-2021-44228 (Log4Shell)
└─ CWE-20 (Improper Input Validation)
└─ CWE-94 (Code Injection)
```

This linkage helps security teams understand **why** a vulnerability exists and how to fix the underlying issue.


### CWE Mitigation Techniques & Best Practices

CWE Weakness	Mitigation Strategy
CWE-79 (XSS)	Use output encoding and CSP headers
CWE-89 (SQLi)	Use parameterized queries
CWE-22 (Path Traversal)	Sanitize input + use file access APIs
CWE-732 (Broken ACLs)	Principle of least privilege

### CWE Scoring for Prioritization

CWE scoring uses:

- **Severity** (Low → Critical)
- **Exploitability** (Remote, local, user interaction)
- **Prevalence** (How often it occurs)
- **Impact** (Confidentiality, Integrity, Availability)

 Tool: CWE Top 25 Most Dangerous Software Weaknesses

 <https://cwe.mitre.org/top25/>



# NVD: National Vulnerability Database

---



## What Is NVD?

- **NVD** is a U.S. government-backed database of **enriched CVEs**
- Adds **analysis, impact scores, and configurations** to raw CVE data

Managed by: **NIST (National Institute of Standards and Technology)**

---



## NVD Data Feeds

Feed Type	What It Contains
CVE Feeds	Enriched CVE info from MITRE
CPE Dictionary	Common Platform Enumeration (e.g., software versions)
CVSS Scores	Impact severity (Base, Temporal, Environmental)
Configuration Feeds	Affected software configs for automation

---



## CVSS: Common Vulnerability Scoring System

---

Used to **rate the severity** of vulnerabilities (0.0 – 10.0)

### CVSS Metrics:

- **Base Score:** How bad is it *in general*?
  - Attack Vector (Local/Network)
  - Attack Complexity
  - Privileges Required
  - User Interaction
  - Scope
  - Impact (C, I, A)
- **Temporal Score:** Exploit code available? Confidence in the report?
- **Environmental Score:** Customizable for your environment



Calculator: <https://nvd.nist.gov/vuln-metrics/cvss>

---



## Using & Integrating NVD Data

---



## Search/Filter Vulnerabilities

Use filters:

- Vendor/Product/Version
- CVSS score range
- CWE type
- Last updated date

Example:

**Find all Apache vulnerabilities with CVSS  $\geq$  8.0 disclosed in 2024**

### **Integrate with Security Tools**

- SIEMs (Splunk, QRadar)
- Vulnerability Scanners (Tenable, Qualys)
- Asset Managers
- Patch Management Tools

They **fetch NVD data** to:

- Identify exposure
  - Prioritize remediation
  - Trigger alerts
-